

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: The ACM Digital Library O The Guide

braid group digitanl signature

Searching within **The ACM Digital Library** for: braid group digitant signature (<u>start a new search</u>) Found **8** of **268**,156

REFINE YOUR SEARCH

E YOUR

Related SIGs
 Related Conferences

•

braid group digitanl sigr

<u>Discovered</u>

Terms

Retine by People

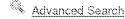
<u>Names</u> <u>Institutions</u> <u>Authors</u>

•

Publication Year
Publication Names
ACM Publications
All Publications
Publishers

Sponsors Events Proceeding Series

ADVANCED SEARCH



FEEDBACK

Please provide us with feedback

Found 8 of 268,156

Results 1 - 8 of 8

Save results to a Binder

Sort by relevance in expanded form

1 One-more matching conjugate problem and security of braid-based signatures

<u>Licheng Wang, Zhenfu Cao, Peng Zeng, Xiangxue Li</u>

March ASI ACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and

2007 communications security **Publisher:** ACM Request Permissions

Full text available: Additional Information: full citation, abstract, references, index terms (KB)

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 49, Downloads (Overall): 210, Citation Count:

Braid groups have recently attracted the attention of many cryptographers as an alternative to number-theoretic public key cryptography. But the published braid-based signatures have failed to reach the most desired security, i.e., existential unforgeability ...

Keywords: braid-based signature, digital signatures, one-more matching conjugate problem, provable security

Quantum resistant public key cryptography: a survey

Ray A. Perlner, David A. Cooper

April IDtrust '09: Proceedings of the 8th Symposium on Identity and Trust on the Internet

2009

2

Publisher: ACM

Full text available: Pdf (359.74 Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 42, Downloads (12 Months): 230, Downloads (Overall): 230, Citation Count: 0

Public key cryptography is widely used to secure transactions over the Internet. However, advances in quantum computers threaten to undermine the security assumptions upon which currently used public key cryptographic algorithms are based. In this paper, ...

Keywords: public key cryptography, quantum computers

3 Vulnerabilities of RFID systems in infant abduction protection and patient wander prevention

Mohamed K. Saad, Syed V. Ahamed

June SI GCSE Bulletin , Volume 39 Issue 2 2007

Publisher: ACM

Full text available: Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 117, Downloads (Overall): 479, Citation Count: 0

This paper presents penetration attacks and abduction drills conducted in a healthcare facility relying on RFID security system to prevent infant abduction and patient wander. The objective is to provide a better understanding to the limitations and ...

Keywords: RFID, infant abduction, protection, vulnerabilities

4 Determining the automorphism group of a hyperelliptic curve

🔌 Tanush Shaska

August ISSAC '03: Proceedings of the 2003 international symposium on Symbolic and algebraic

2003 computation

Publisher: ACM & Request Permissions

Full text available: Pdf (250.89 KR) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 30, Downloads (Overall): 286, Citation Count: 1

In this note we discuss techniques for determining the automorphism group of a genus \$g\$ hyperelliptic curve \$\X_g\$ defined over an algebraically closed field \$k\$ of characteristic zero. The first technique uses the classical \$GL_2 (k)\$-invariants of ...

Keywords: automorphism, hyperelliptic curve, moduli space

5 Audio hallway: a virtual acoustic environment for browsing

Chris Schmandt

November UIST '98: Proceedings of the 11th annual ACM symposium on User interface software and

1998 technology

Publisher: ACM Request Permissions

Full text available: Full (65.62 KB)

Additional Information: full citation, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 35, Downloads (Overall): 424, Citation Count: 9

Keywords: auditory user interface, digitized speech, spatial audio, virtual enviroments

6 Online pairing of VoIP conversations

Michail Vlachos, Aris Anagnostopoulos, Olivier Verscheure, Philip S. Yu

January The VLDB Journal — The International Journal on Very Large Data Bases, Volume 18

2009 Issue 1

Publisher: Springer-Verlag New York, Inc.

Full text available: Pdf (1.53 MB)

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 16, Downloads (12 Months): 89, Downloads (Overall): 89, Citation Count: 0

This paper answers the following question; given a multiplicity of evolving 1-way conversations, can a machine or an algorithm discern the conversational pairs in an online fashion, without understanding the content of the communications? Our analysis ...

Keywords: Binary time-series clustering, Conversation pairing, Stream clustering, Voice-over-IP Information security issues in an APL application

Bill Hillman

June 1984 APL '84: Proceedings of the international conference on APL

Publisher: ACM

Full text available: [Fold (549.98] Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 12, Downloads (12 Months): 24, Downloads (Overall): 258, Citation Count: 0

This paper will describe various methods to secure an APL database application. Primary foci will be in the areas of "physical" protection, and in cryptographic techniques. To that end, distinctions will be made between "data," ...

Also published in:

June 1984 SIGAPL APL Quote Quad Volume 14 Issue 4

8 ACM SIGSAM Bulletin: Volume 39 Issue 1

March 2005 SIGSAM Bulletin

Publisher: ACM

Additional Information: full citation, index terms

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count: 0

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2010 ACM, Inc.

Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player